NIA PRESENTATION

MINIMUM INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY IN THE GOVERNMENT ENVIRONMENT

SEPTEMBER 2007
TOPICS

1. State of security
2. Legislation framework
   - MISS
   - New act, regulations and standards
3. ICT incidences, reasons and threats in the government environment
4. Way forward and conclusion
STATE OF SECURITY

A WEAK LINK

LACK OF SECURITY
The general lack of security at government departments, parastatals and national strategic key points remains one of the most serious security threats facing government. A slight improvement has occurred in terms of institutions’ general compliance with security prescriptions, following the result of security interventions during the past year. Government departments and institutions’ general state of security vulnerability continues to be highlighted by security breaches at high-profile departments and a range of parastatals, institutions and installations. In some cases the breaches were accompanied by a loss of computer equipment containing sensitive information.
LEGISLATION FRAMEWORK

A WEAK LINK

LACK OF SECURITY
CURRENT NATIONAL POLICY: MISS

- An acronym for “Minimum Information Security Standards”
- National information security policy, approved by Cabinet on 4 December 1996
- A guideline to HOD/CEO to draft departmental/ internal Security Policy & Directives
- Don’t give proper guidance to ICT environment
- Direct institutions how to implement security – See handout (14 COMPLIANCE INDICATORS)
LEGISLATION: NEW ACT & REGULATIONS

• Regulate the manner in which state information may be protected;
• Promote transparency and accountability in governance while recognizing that information may be protected from disclosure in order to safeguard the national interest;
• Establish general principles in terms of which state information may be handled and protected in a constitutional democracy;
• Provide a regulatory framework in terms of which protected information is safeguarded in accordance with national and departmental policies and procedures;
• Define the nature and categories of information that may be protected from destruction, loss and/or unauthorized disclosure;
The Minister of Intelligence may make regulations to provide for:

- the controls and measures required to effectively protect information;
- the responsibilities of heads of an organ of state;
- the organization and administration of the ICT function at organs of state; (See Chapter 11)
- a personnel security clearance system;
- restrictions on how classified information may be transferred;
- the reporting of security breaches at organs of state; (See handout regarding Regulation)
INCIDENCES IN THE GOVERNMENT ENVIRONMENT

A WEAK LINK

LACK OF SECURITY
Some of the more common examples in this regard include

- Non-adherence to prescriptions in terms of information security, for instance improper handling, storage and/or transmission of classified and/or sensitive information,
- Inadequate key control and non-adherence to ICT access procedures (e.g. computers not logged off after hours), thus facilitating unauthorised access to classified or sensitive information.
- The non-adherence to prescribed access procedures is especially problematic because it provides unimpeded access to classified and sensitive information via electronic means.
COMPUTERS AND PARTS PRIME TARGET
LOG OUT OF NETWORK WHEN LEAVING OFFICE
SECURITY INCIDENCES REASONS

• Most security incidences had definite elements in common, principal of which were
  • Inadequacies in terms of physical security measures.
  • Lack of security consciousness and awareness among personnel of the affected institutions.
  • Lack of security commitment by individuals in structures.
  • Lack of integrity towards Government.
  • Non vetting of staff and contractors in sensitive positions.
COMMON THREATS AND RISKS:
• No Internal policy and/or directives
• Contractors or Service providers not vetted
• Passwords and management thereof
• Social engineering (Pretexting, Phishing, etc.)
• Insecure modems
• Internet security
• E-mail
• Malware
• Hard drives – permanent storage
• Removable media
• Laptops
WAY FORWARD AND CONCLUSION

A WEAK LINK

LACK OF SECURITY
WHAT IS NEEDED?

• Institutions must have focused security programs for employees and management to protect information from theft or compromise
• Employee awareness of the problem, alertness to indicators of suspicious activity, and willingness to report those indicators to management are keys to the successful protection of information
• The security program should consist of the following seven elements:
  • Security organisation (Manager, Committee, etc)
  • Security administration (policies, information security officer(s))
  • Information security
  • Personnel security
  • Physical security
  • ICT security (encryption, management, etc.)
  • BCP
WHAT IS NEEDED? Cont.

- Implement real-time system monitoring and reporting mechanisms
- Perform integrity checks on system software;
- Check for configuration vulnerabilities;
- Conduct security audits of information and communication technology assets
THANK YOU